Chapter 6
Multi-round Box

In the previous chapter we discussed the *single-round box*, which can be seen as a simple abstract object that allows us to study the fundamental aspects of non-locality. When studying actual device-independent information processing tasks, however, one must consider more complex objects that describe the behaviour of the devices while performing the task of interest. More concretely, in actual applications we usually interact with a device by playing *many* games. Even in the simplest setting where one would like to merely verify the violation of a Bell inequality, as in experiments performing loophole-free Bell tests, a Bell game is played many times so that sufficient amount of data can be collected to estimate the violation in a satisfactory statistical manner. Playing just a single game is clearly not enough. Another example is device-independent protocols, such as quantum key distribution. All protocols include a phase in which the users (or honest parties) are playing many games with their device in order to decide whether it can be used for the considered task. Hence, considering boxes that can be used to play just a single game is not enough. Instead, we need to work with *multi-round boxes*.

Multi-round boxes can be described using a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ over the inputs and outputs of many rounds of a game. That is, for n the number of games which one would like to play with the box (e.g., the number of rounds of a protocol), $\boldsymbol{A} = A_1 A_2 \ldots A_n$ is a random variable over $\mathcal{A}^n$ and $\boldsymbol{B}$, $\boldsymbol{X}$, and $\boldsymbol{Y}$ are similarly defined.

As explained in the beginning of Chap. 5, the way we model a box, and in particular a multi-round box, depends on the type of interaction that we would like to perform with it. We consider two different forms of interactions: parallel and sequential interactions. Different tasks require different types of boxes. Parallel boxes are used, for example, in self-testing [1], parallel quantum key distribution [2], and certification of entanglement [3]. Some examples for settings in which sequential boxes

R. Arnon-Friedman, *Device-Independent Quantum Information Processing*,
Springer Theses, https://doi.org/10.1007/978-3-030-60231-4_6

are considered are delegated computation [4] and randomness amplification [5]. In the scope of this thesis, Chaps. 8 and 10 deal with parallel boxes while Chaps. 9 and 11 focus on sequential boxes.

6.1 Parallel Interaction

The simplest to describe form of interaction is the "parallel interaction". In such an interaction the box is "expecting" to get the n inputs of all the rounds, $\boldsymbol{x}$ and $\boldsymbol{y}$, at the same time and is expected to give all the outputs, $\boldsymbol{a}$ and $\boldsymbol{b}$, together; see Fig. 6.1. If the box is only given inputs of a single game, e.g., x_1, y_1, it is not expected to return any output. This behaviour of the box will present itself in the mathematical model of the box, as we explain below.

For a given a game G, a parallel multi-round box is a device with which Alice and Bob can play n instances of G in parallel (i.e., at the same time). Mathematically this translates to a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$, non-signalling between Alice and Bob, defined over the inputs and outputs of n games. For example, when considering the CHSH game, $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{X}$, and $\boldsymbol{Y}$ are all random variables over $\{0, 1\}^n$.

As explained in Sect. 3.1.1, the non-signalling conditions between Alice and Bob imply that Alice and Bob's marginals, $\mathrm{P}_{\boldsymbol{A}|\boldsymbol{X}}$ and $\mathrm{P}_{\boldsymbol{B}|\boldsymbol{Y}}$ respectively, are well-defined. The fact that we are talking about a *parallel* multi-round box means that no further structure can be assumed. In particular, other marginals, e.g., $\mathrm{P}_{A_1|X_1}$ or $\mathrm{P}_{A_2B_2|X_2B_2}$, are not necessarily well-defined. Intuitively this stands for the fact that the box is expecting to get all the inputs together and only then it produces the outputs; the output for A_1 can therefore depend, for example, on the value of X_5 and not on

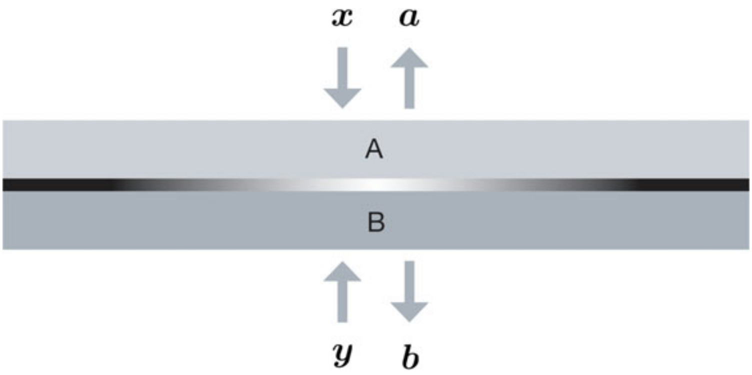

Fig. 6.1 Parallel multi-round box. We think of a parallel multi-round box as a large device, shared between Alice and Bob, which can be used to play many rounds of a Bell game, all at once. Such a box is expecting to get the inputs for all rounds, $\boldsymbol{x}$ and $\boldsymbol{y}$, at the same time, and it will then produce all the outputs, $\boldsymbol{a}$ and $\boldsymbol{b}$ for Alice and Bob

just that of X_1. Hence the conditional probability distribution $\mathrm{P}_{A_1|X_1}$ is not properly defined.

6.1.1 Non-signalling Parallel Boxes

One can consider a parallel multi-round box which is only restricted by the non-signalling conditions. We then get the following definition.

Definition 6.1 (*Non-signalling parallel multi-round box*) Given a Bell game G, a non-signalling parallel multi-round box is a non-signalling box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$, as in Definition 3.1, defined for the inputs and outputs of n rounds of the game G – $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$. That is, for all $\boldsymbol{a} \in \mathcal{A}^n$, $\boldsymbol{b} \in \mathcal{B}^n$, $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}^n$ and $\boldsymbol{y}, \boldsymbol{y}' \in \mathcal{Y}^n$,

$$\begin{aligned}\sum_{\boldsymbol{b}} \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{ab}|\boldsymbol{x}\boldsymbol{y}) &= \sum_{\boldsymbol{b}} \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{ab}|\boldsymbol{x}\boldsymbol{y}') \\ \sum_{\boldsymbol{a}} \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{ab}|\boldsymbol{x}\boldsymbol{y}) &= \sum_{\boldsymbol{a}} \mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{ab}|\boldsymbol{x}'\boldsymbol{y}) \ .\end{aligned} \tag{6.1}$$

As mentioned above, the only non-signalling conditions restricting the parallel box, are those between Alice and Bob appearing in Definition 6.1; we do not set any other assumptions regarding the box apart from that.

6.1.1.1 Quantum Parallel Boxes

Similarly to a quantum single-round box, as in Definition 5.1, a quantum parallel multi-round box is just a quantum box (Definition 3.3) defined for the inputs and outputs of n rounds of G.

Definition 6.2 (*Quantum parallel multi-round box*) Given a Bell game G, a quantum parallel multi-round box is a quantum box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$, as in Definition 3.3, defined for the inputs and outputs of n rounds of the game G – $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$. That is, there exist a bipartite state $\rho_{Q_A Q_B}$ and measurements $\{M_{\boldsymbol{a}}^{\boldsymbol{x}}\}$ and $\{M_{\boldsymbol{b}}^{\boldsymbol{y}}\}$ such that

$$\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}(\boldsymbol{ab}|\boldsymbol{x}\boldsymbol{y}) = \mathrm{Tr}\left(M_{\boldsymbol{a}}^{\boldsymbol{x}} \otimes M_{\boldsymbol{b}}^{\boldsymbol{y}}\ \rho_{Q_A Q_B}\right) \quad \forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \ . \tag{6.2}$$

The non-signalling conditions in Eq. (6.1) are automatically fulfilled by quantum parallel boxes defined above. We remark again that there are no further assumptions regarding the structure of the state and measurements apart from what appears in Eq. (6.2). Specifically, ρ_{Q_A} and ρ_{Q_B} are not assumed to have some further subsystem structure and the measurements need not have a tensor product form such as $M_{a_1}^{x_1} \otimes \cdots \otimes M_{a_n}^{x_n}$.

6.2 Sequential Interaction

In the previous section we discussed *parallel* multi-rounds boxes. These are boxes that allow (and "expect") to be interacted with in a parallel way, i.e., by giving all the inputs to the box at the same time. As the parallel multi-round box receives all the inputs at once, the output for, e.g., the first game, A_1, can depend on the inputs for all games $X_1, X_2, \ldots, X_n$.

In this section we consider a different type of multi-round boxes – *sequential multi-round boxes*. Such boxes are, in some sense, more structured than parallel multi-round boxes and accurately model the devices used in many device-independent scenarios. As such, sequential multi-round boxes are of relevance for applications. Furthermore, the additional structure of sequential multi-round boxes will allow us to derive stronger results than those derived for their parallel counterparts.

As mentioned above, the way we model a multi-round box depends on how we would like to interact with it. Most device-independent protocols proceed in rounds which are performed one after the other: Alice and Bob use their box in the first round of the protocol and only once they receive the outputs from the box they proceed to the second round, and so on; See Protocol 1.1 for an example. We call such an interaction with the box "sequential interaction". This is illustrated in Fig. 6.2 (the reader may compare Fig. 6.2 to the single-round box in Fig. 5.1 and the parallel multi-round box in Fig. 6.1).

The chronological order which is implied by the sequential interaction enforces certain constraints on the behaviour of the box. In particular, while past events can influence future ones, the future cannot change the past. For example, the first output A_1 can depend on the first input X_1 but not on the inputs of the next rounds $X_2, \ldots, X_n$. The second output A_2 can depend both on X_2 and past events, such as the values assigned to A_1 and X_1, but not on the following inputs $X_3, \ldots, X_n$.

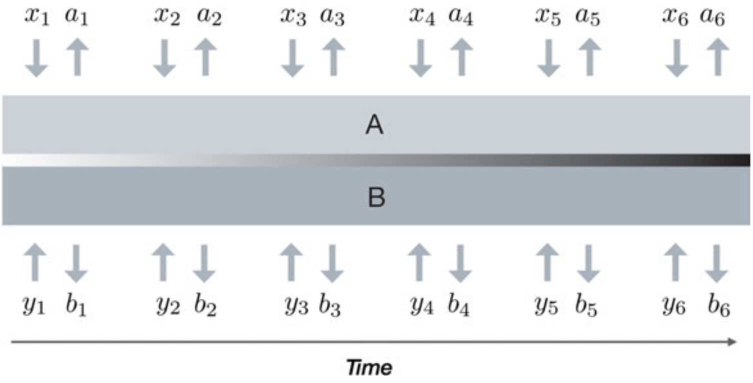

Fig. 6.2 Sequential interaction with a multi-round box. Alice and Bob start by playing the first game with the box and only once they receive the outputs from the box they proceed to the second game, and so on

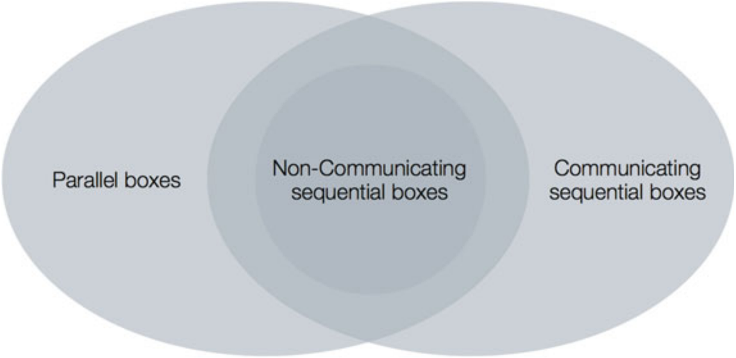
Parallel boxes
Non-Communicating sequential boxes
Communicating sequential boxes

Fig. 6.3 The relation between the different multi-round boxes

We define two different types of sequential boxes – one which allows for communication between the rounds of interactions and one which does not. A box that allows for communication between the rounds is a box in which Alice and Bob's devices can exchange classical or quantum information after finishing playing a game and before starting the next one. Such boxes should be considered when entanglement is to be distributed "on the fly", e.g., in protocols where Alice is expected to send half of an entangled state to Bob in each round, or when the devices are located far enough so they cannot communicate during a *single* game but too close to make sure signals from one round cannot arrive to the other device until the end of *all* games. A box that does not allow for communication can be considered, e.g., in cryptographic settings in which any communication between the devices implies that *all* information can leak to the adversary. We remark that parallel boxes and sequential boxes that allow for communications are incomparable to one another, while both are more general than sequential boxes without communication; see Fig. 6.3. This is explained in more detail after formally defining the two types of sequential boxes.

6.2.1 Without Communication Between the Rounds

As in the case of a parallel multi-round box, a sequential multi-round box is described by a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ defined over the inputs and outputs of n rounds of the game $\mathrm{G} - \mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$. The special thing about a sequential box is that the marginals describing the individual rounds of the game are well-defined and non-signalling between Alice and Bob. That is, they are boxes by themselves.

In this section we consider a model of sequential boxes in which Alice's and Bob's components are not allowed to communicate between the rounds of the game. For short, we call such boxes *non-communicating sequential boxes*. Formally, to define a non-communicating sequential box we consider the marginals of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ describing a round $i \in [n]$. The relevant marginals are

$$\mathrm{P}_{A_i B_i|X_i Y_i H^{i,\mathrm{Alice}} H^{i,\mathrm{Bob}}} \tag{6.3}$$

where $H^{i,\mathrm{Alice}} = \boldsymbol{X}_{1,\ldots,i-1}\boldsymbol{A}_{1,\ldots,i-1}$ and $H^{i,\mathrm{Bob}} = \boldsymbol{Y}_{1,\ldots,i-1}\boldsymbol{B}_{1,\ldots,i-1}$ denote the "histories" of Alice and Bob's boxes in round i. These histories basically describe all the information that can be kept by the boxes from the previous rounds (we can think of such boxes as devices which record past events in their memory). The history may include more information[1] than past inputs and outputs; for simplicity we stick to the above choice.

A first requirement on a sequential box is that the marginals (6.3) are well-defined. This can be mathematically described by a set of non-signalling conditions. Explicitly, for every $i \in [n]$, we denote:

1. $\mathcal{P} = [i-1]$, $\boldsymbol{a}_{\mathcal{P}} = a_1, \ldots, a_{i-1}$, and similarly for $\boldsymbol{b}_{\mathcal{P}}$, $\boldsymbol{x}_{\mathcal{P}}$, and $\boldsymbol{y}_{\mathcal{P}}$.
2. $\mathcal{F} = \{i+1, \ldots, n\}$, $\boldsymbol{a}_{\mathcal{F}} = a_{i+1}, \ldots, a_n$, and similarly for $\boldsymbol{b}_{\mathcal{F}}$, $\boldsymbol{x}_{\mathcal{F}}$, and $\boldsymbol{y}_{\mathcal{F}}$.
3. For any $\boldsymbol{x}_{\mathcal{P}}$, $\boldsymbol{y}_{\mathcal{P}}$, x_i, y_i, $\boldsymbol{x}_{\mathcal{F}}$, $\boldsymbol{y}_{\mathcal{F}}$, $\boldsymbol{x}'_{\mathcal{F}}$, and $\boldsymbol{y}'_{\mathcal{F}}$,

   (a) $\boldsymbol{x} = \boldsymbol{x}_{\mathcal{P}}, x_i, \boldsymbol{x}_{\mathcal{F}}$
   (b) $\boldsymbol{x}' = \boldsymbol{x}_{\mathcal{P}}, x_i, \boldsymbol{x}'_{\mathcal{F}}$

   and similarly for $\boldsymbol{y}$ and $\boldsymbol{y}'$.

Then, we require that the following non-signalling conditions hold for all $\boldsymbol{a}_{\mathcal{P}}$, $\boldsymbol{b}_{\mathcal{P}}$, $\boldsymbol{x}_{\mathcal{P}}$, $\boldsymbol{y}_{\mathcal{P}}$, a_i, b_i, x_i, y_i, $\boldsymbol{x}_{\mathcal{F}}$, $\boldsymbol{x}'_{\mathcal{F}}$, $\boldsymbol{y}_{\mathcal{F}}$, and $\boldsymbol{y}'_{\mathcal{F}}$,

$$\begin{aligned} &\sum_{\boldsymbol{a}_{\mathcal{F}}, \boldsymbol{b}_{\mathcal{F}}} \mathrm{P}_{A_i B_i \boldsymbol{A}_{\mathcal{F}} \boldsymbol{B}_{\mathcal{F}} | \boldsymbol{A}_{\mathcal{P}} \boldsymbol{B}_{\mathcal{P}} \boldsymbol{X}\boldsymbol{Y}} \left(a_i, b_i, \boldsymbol{a}_{\mathcal{F}}, \boldsymbol{b}_{\mathcal{F}} | \boldsymbol{a}_{\mathcal{P}}, \boldsymbol{b}_{\mathcal{P}}, \boldsymbol{x}, \boldsymbol{y}\right) = \\ &\qquad \sum_{\boldsymbol{a}_{\mathcal{F}}, \boldsymbol{b}_{\mathcal{F}}} \mathrm{P}_{A_i B_i \boldsymbol{A}_{\mathcal{F}} \boldsymbol{B}_{\mathcal{F}} | \boldsymbol{A}_{\mathcal{P}} \boldsymbol{B}_{\mathcal{P}} \boldsymbol{X}\boldsymbol{Y}} \left(a_i, b_i, \boldsymbol{a}_{\mathcal{F}}, \boldsymbol{b}_{\mathcal{F}} | \boldsymbol{a}_{\mathcal{P}}, \boldsymbol{b}_{\mathcal{P}}, \boldsymbol{x}', \boldsymbol{y}'\right) . \end{aligned} \tag{6.4}$$

Now that the marginals $\mathrm{P}_{A_i B_i|X_i Y_i H^{i,\mathrm{Alice}} H^{i,\mathrm{Bob}}}$ are well-defined for all $i \in [n]$, we further ask that they are non-signalling between Alice and Bob, when each party holds only its own history. That is, $\mathrm{P}_{A_i|X_i H^{i,\mathrm{Alice}}}$ and $\mathrm{P}_{B_i|Y_i H^{i,\mathrm{Bob}}}$ need to be well-defined as well. Explicitly, for each round $i \in [n]$, for all $a \in \mathcal{A}, b \in \mathcal{B}, x, x' \in \mathcal{X},\ y, y' \in \mathcal{Y}$ and histories $h^{i,\mathrm{Alice}}, h^{i,\mathrm{Alice}'} \in \mathcal{X}^{i-1} \times \mathcal{A}^{i-1}$ and $h^{i,\mathrm{Bob}}, h^{i,\mathrm{Bob}'} \in \mathcal{Y}^{i-1} \times \mathcal{B}^{i-1}$,

$$\begin{aligned} &\sum_b \mathrm{P}_{A_i B_i|X_i Y_i H^{i,\mathrm{Alice}} H^{i,\mathrm{Bob}}}(a, b|x, y, h^{i,\mathrm{Alice}}, h^{i,\mathrm{Bob}}) = \\ &\qquad \sum_b \mathrm{P}_{A_i B_i|X_i Y_i H^{i,\mathrm{Alice}} H^{i,\mathrm{Bob}}}(a, b|x, y', h^{i,\mathrm{Alice}}, h^{i,\mathrm{Bob}'}) \\ &\sum_a \mathrm{P}_{A_i B_i|X_i Y_i H^{i,\mathrm{Alice}} H^{i,\mathrm{Bob}}}(a, b|x, y, h^{i,\mathrm{Alice}}, h^{i,\mathrm{Bob}}) = \\ &\qquad \sum_a \mathrm{P}_{A_i B_i|X_i Y_i H^{i,\mathrm{Alice}} H^{i,\mathrm{Bob}}}(a, b|x', y, h^{i,\mathrm{Alice}'}, h^{i,\mathrm{Bob}}) . \end{aligned} \tag{6.5}$$

[1] For example, in device-independent quantum key distribution protocols the parties randomly choose in each round whether the round is used for testing the device or for generating key bits. This information can also be included in the history H^i.

The fact that the boxes cannot communicate between the rounds presents itself by having two different histories, one for Alice and one for Bob. The above equations then imply that the actions of Alice's box in round i depend only on Alice's history, i.e., on what happened in the previous rounds on Alice's side (while she is oblivious to Bob's history), and similarly for Bob.[2]

Note that we only ask the marginals $\mathrm{P}_{A_i|X_i H^{i,\mathrm{Alice}}}$ and $\mathrm{P}_{B_i|Y_i H^{i,\mathrm{Bob}}}$ to be well-defined. $\mathrm{P}_{A_i|X_i}$, on the other hand, are not necessarily valid boxes.

6.2.1.1 Non-signalling Non-communicating Sequential Boxes

A non-signalling non-communicating sequential multi-round box is simply a box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ fulfilling the above non-signalling constraints; there are no further requirements.

Definition 6.3 (*Non-signalling non-communicating sequential multi-round box*) Given a Bell game G, a non-signalling non-communicating sequential multi-round box is a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ defined for the inputs and outputs of n rounds of the game G – $\mathcal{X}^n$, $\mathcal{Y}^n$, $\mathcal{A}^n$, $\mathcal{B}^n$ fulfilling the non-signalling conditions given in Eqs. (6.4) and (6.5).

6.2.1.2 Quantum Non-communicating Sequential Boxes

The simplest way of defining a quantum non-communicating sequential box is to consider the initial state shared by Alice and Bob and the sequence of measurements that they perform.

More specifically, in each round Alice and Bob's boxes can perform a measurement on the post-measurement state of the previous round. We denote the state in the beginning of round $i \in [n]$ (i.e., before performing the measurements of the i'th round) by $\rho_{Q_A Q_B}^{i,h^{i,\mathrm{Alice}},h^{i,\mathrm{Bob}}}$. As clear from the notation, this state depends on the histories $h^{i,\mathrm{Alice}}$, $h^{i,\mathrm{Bob}}$. We identify $\rho^1_{Q_A Q_B} = \rho_{Q_A Q_B}$ as the initial state of the box.

Furthermore, we denote the (Kraus) measurements performed in each round by $\{K_a^x\}$ and $\{K_b^y\}$.[3] One can think of the measurements $\{K_a^x\}$ as depending on the history $h^{i,\mathrm{Alice}}$ and similarly for Bob. Alternatively, we can imagine that the history is already kept in some classical registers within the quantum state $\rho_{Q_A Q_B}^{i,h^{i,\mathrm{Alice}},h^{i,\mathrm{Bob}}}$, i.e., ρ_{Q_A} includes also the information $h^{i,\mathrm{Alice}}$ and similarly for Bob. The measurements can thus be defined as first reading the history and then applying the relevant measurement depending on the history. This allows us to use the shorter notation in which the operators do not depend on the histories explicitly.

[2] This should be compared to the next section, where we will have just a single history H^i for Alice and Bob together.

[3] Note that in contrast to the previous definitions, the measurement operators K are now written as Kraus operators and not POVMs, since we are interested in the post-measurement state. See Sect. 2.3 for more details.

Using the above notation, the relation between the state in round i to that of round $i-1$ is simply (up to normalisation of the state)

$$\rho_{Q_A Q_B}^{i,h^{i,\text{Alice}},h^{i,\text{Bob}}} \propto \left(K_{a_{i-1}}^{x_{i-1}} \otimes K_{b_{i-1}}^{y_{i-1}}\right) \rho_{Q_A Q_B}^{i-1,h^{i-1,\text{Alice}},h^{i-1,\text{Bob}}} \left(\left(K_{a_{i-1}}^{x_{i-1}}\right)^{\dagger} \otimes \left(K_{b_{i-1}}^{y_{i-1}}\right)^{\dagger}\right) , \tag{6.6}$$

where $h^{i,\text{Alice}}$ and $h^{i,\text{Bob}}$ uniquely determine $x_{i-1}, a_{i-1}, h^{i-1,\text{Alice}}$ and $y_{i-1}, b_{i-1}, h^{i-1,\text{Bob}}$, respectively (i.e., the values on the righthand-side of Eq. (6.6) should be consistent with the histories on the lefthand-side). The conditions stated in Eq. (6.5) follow directly.

Definition 6.4 (*Quantum non-communicating sequential multi-round box*) Given a Bell game G, a quantum non-communicating sequential multi-round box is a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ defined for the inputs and outputs of n rounds of the game G, $\mathcal{X}^n, \mathcal{Y}^n, \mathcal{A}^n, \mathcal{B}^n$, such that there exist a bipartite state $\rho_{Q_A Q_B}$ and measurements $\{K_a^x\}$ and $\{K_b^y\}$ defining a sequence of bipartite states for $i \in [n]$ as in Eq. (6.6).

As mentioned before, a non-communicating sequential box is also a parallel one. Indeed, it is easy to see that a parallel box can always simulate the behaviour of a non-communicating sequential box.

6.2.2 With Communication Between the Rounds

In the previous section we considered sequential boxes in which Alice's and Bob's components are not allowed to communicate between the rounds. This implies that Alice's and Bob's components evolve separately in time and each of them has their own "history": $h^{i,\text{Alice}}$ for Alice and $h^{i,\text{Bob}}$ for Bob. Now, we consider a scenario in which Alice's and Bob's components are allowed to communicate between the different games, i.e., after the outputs of round $i-1$ were supplied by the box and before the i'th inputs are given.[4] Considering boxes that are allowed to communicate is, in particular, relevant when considering realistic application of, e.g., device-independent cryptography. There, one would like to allow the experimentalists to distribute entanglement "on the fly" during the protocol. To send a new quantum state in each round the communication channels need to be open and an adversarial box may use this opportunity to communicate.

Mathematically this setting can be formalised by allowing Alice and Bob to keep a common history register that includes the classical information of all past events *on both sides*. More specifically, the marginal describing the i'th round of the game,

[4] In Protocol 1.1, for example, "between the different games" refers to the time *after* Step 3 of round $i-1$ and *before* Step 2 of round i, for all $i \in [n]$.

for $i \in [n]$, is given by $\mathrm{P}_{A_i B_i|X_i Y_i H^i}$, where H^i denotes the history defined by the previous rounds. H^i includes $\boldsymbol{X}_{1,\dots,i-1}\boldsymbol{Y}_{1,\dots,i-1}\boldsymbol{A}_{1,\dots,i-1}\boldsymbol{B}_{1,\dots,i-1}$ as well as any other information available to Alice's and Bob's component. For simplicity we assume that $H^i = \boldsymbol{X}_{1,\dots,i-1}\boldsymbol{Y}_{1,\dots,i-1}\boldsymbol{A}_{1,\dots,i-1}\boldsymbol{B}_{1,\dots,i-1}$ similarly to what was done before. The only non-trivial communication to consider is one which depends on the history, since any other information could have been included as part of the box to begin with. Therefore, we can assume without loss of generality that the communicated information is simply the entire history.

As before, we first require that $\mathrm{P}_{A_i B_i|X_i Y_i H^i}$ are well-defined, i.e., Eq. (6.4) is fulfilled. In addition, $\mathrm{P}_{A_i B_i|X_i Y_i H^i}$ needs to be non-signalling between Alice and Bob, when they both hold their common history. That is, $\mathrm{P}_{A_i|X_i H^i}$ and $\mathrm{P}_{B_i|Y_i H^i}$ are well-defined. Formally: for each round $i \in [n]$, for all $a \in \mathcal{A}, b \in \mathcal{B}, x, x' \in \mathcal{X},\ y, y' \in \mathcal{Y}$ and $h^i \in \mathcal{A}^{i-1} \times \mathcal{B}^{i-1} \times \mathcal{X}^{i-1} \times \mathcal{Y}^{i-1}$,

$$\begin{aligned}\sum_b \mathrm{P}_{A_i B_i|X_i Y_i H^i}(a, b|x, y, h^i) &= \sum_b \mathrm{P}_{A_i B_i|X_i Y_i H^i}(a, b|x, y', h^i)\\ \sum_a \mathrm{P}_{A_i B_i|X_i Y_i H^i}(a, b|x, y, h^i) &= \sum_a \mathrm{P}_{A_i B_i|X_i Y_i H^i}(a, b|x', y, h^i)\ .\end{aligned} \tag{6.7}$$

In contrast to Eq. (6.5), in the above equations the behaviour of Alice's component in the i'th round may depend also on past events on Bob's side, as H^i includes also $\boldsymbol{Y}_{1,\dots,i-1}\boldsymbol{B}_{1,\dots,i-1}$, and similarly for Bob's part of the box.

6.2.2.1 Non-signalling Communicating Sequential Boxes

A non-signalling communicating sequential multi-round box is a box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ fulfilling the above non-signalling constraints.

Definition 6.5 (*Non-signalling communicating sequential multi-round box*) Given a Bell game G, a non-signalling communicating sequential multi-round box is a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ defined for the inputs and outputs of n rounds of the game G – $\mathcal{X}^n$, $\mathcal{Y}^n$, $\mathcal{A}^n$, $\mathcal{B}^n$ fulfilling the non-signalling conditions given in Eqs. (6.4) and (6.7).

It is perhaps instructive to note that $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ itself is *not* a non-signalling box.; communication (i.e., signalling) between the rounds may be *necessary* in order to implement the box. We give a trivial example in the end of the section.

6.2.2.2 Quantum Communicating Sequential Boxes

When we say that a communicating sequential multi-round box is quantum we mean that in each round the behaviour of the box can be described within the formalism of quantum physics.

Definition 6.6 (*Quantum communicating sequential multi-round box*) Given a Bell game G, a quantum sequential multi-round box is a conditional probability distribution $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ defined for the inputs and outputs of n rounds of the game G, $\mathcal{X}^n$, $\mathcal{Y}^n$, $\mathcal{A}^n$, $\mathcal{B}^n$, such that for all $i \in [n]$ the marginal $\mathrm{P}_{A_i B_i | X_i Y_i H^i}$, for $H^i = \boldsymbol{X}_{1,\dots,i-1}$ $\boldsymbol{Y}_{1,\dots,i-1} \boldsymbol{A}_{1,\dots,i-1} \boldsymbol{B}_{1,\dots,i-1}$, is a quantum box as in Definition 3.3. That is, there exist a bipartite state $\rho^{h^i}_{Q_A Q_B}$ and measurements $\{M_a^{h^i,x}\}$ and $\{M_b^{h^i,y}\}$ such that

$$\mathrm{P}_{A_i B_i | X_i Y_i H^i}(ab|xyh^i) = \mathrm{Tr}\left(M_a^{h^i,x} \otimes M_b^{h^i,y} \ \rho^{h^i}_{Q_A Q_B} \right) \quad \forall a, b, x, y, h^i \ . \tag{6.8}$$

The box in Eq. (6.8) is written as $\mathrm{P}_{A_i B_i | X_i Y_i H^i}$ so it is mathematically clear which marginals of $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$ are being discussed. On the level of the state and measurements one thinks of $\rho^{h^i}_{Q_A Q_B}$, $\{M_a^{h^i,x}\}$, and $\{M_b^{h^i,y}\}$ as depending on the history h^i, which allows the actions in each round to depend on the past. As in Sect. 6.2.1, we may also consider a state $\rho^{h^i}_{Q_A Q_B}$ that keeps h^i in one of its registers and measurements that first read the history and then apply the relevant operations; in such a case we may think of $\{M_a^x\}$, and $\{M_b^y\}$ independent of the history.

It may seem from Definition 6.6 that only the individual rounds are considered. The sequential nature of the box is concealed in the relations between the different rounds. It becomes apparent when noting that all the marginals describing the individual rounds should be consistent with the same overall box $\mathrm{P}_{\boldsymbol{AB}|\boldsymbol{XY}}$. Alternatively, one can consider an equivalent definition of a quantum communicating sequential multi-round box that is perhaps more intuitive (but mathematically more complex): Similarly to the evolution described in Eq. (6.6), we start with some initial quantum state and make sequential measurements. In contrast to Eq. (6.6), however, we allow for an additional general operation, which may depend on the history, to be performed on the post-measurement state of each round. The general operation between the rounds is what models the communication between the two parts of the box.

Before concluding this section, let us mention the relations between the different types of multi-round boxes. The relations are shown in Fig. 6.3. It is obvious to see that communicating sequential boxes are more general than non-communicating sequential boxes. In contrast to non-communicating sequential boxes, parallel boxes cannot simulate a general communicating sequential box. A trivial example is a communicating sequential box that always outputs $b_2 = x_1$. Clearly, since a parallel box must, in particular, fulfill Eq. (6.1), it cannot simulate such a box. On the other hand, communicating sequential boxes cannot simulate a general parallel box. For example, a communicating sequential box cannot simulate a parallel box for which $a_1 = x_2$. Thus, the two types of boxes are incomparable.

References

1. Natarajan A, Vidick T (2017) A quantum linearity test for robustly verifying entanglement. In: Proceedings of the 49th annual ACM SIGACT symposium on theory of computing. ACM, pp. 1003–1015
2. Jain R, Miller CA, Shi Y (2017) Parallel device-independent quantum key distribution. arXiv preprint arXiv:1703.05426
3. Arnon-Friedman R, Yuen H (2018) Noise-tolerant testing of high entanglement of formation. Int Coll Autom, Lang, Program
4. Reichardt BW, Unger F, Vazirani U (2013) Classical command of quantum systems. Nature 496(7446):456–460
5. Kessler M, Arnon-Friedman R (2017) Device-independent randomness amplification and privatization. arXiv preprint arXiv:1705.04148